Analysis of Privacy Policy: Responses and Challenges. "Experiences from Service Providers"

Murtaza Hussain Shaikh, *Member, IACSIT*

***Abstract*—The main purpose of this paper is to investigate how different the service provider's point of view about understandability, technicality, importance and awareness of privacy policy. The emerging ambiguity in information security has raised much privacy and trust issues that are context dependent. Therefore there are several uncertainties and risks seen today concerning the privacy policy and subscriber trust. It is a responsibility of services providers before amending their policy to notify their subscribers. Because if they do not take this initiative then it creates trust deficit for their subscribers and this affects their business and goodwill. In this work we have adopted the online survey questionnaire technique to perform a research based on the organization's own perspectives on the privacy policy. This would highlight to what extent and organizations think the policy fulfills the user's confidence. We have decided to target Norwegian service providers for this survey, to better understand the theme of research. Generally observed in this work is that, before accepting privacy policy, it is hard to read these policies and understood by end-user, and taking this prospect ahead, many privacy policies and regulations have a difficult context to understand.**

***Index Terms*—Privacy, personal information, service providers, subscriber`s policy, issues, survey design, legislation, settings, practices, information security concerns.**

I. Introduction

More than a century ago, Warren and Brandeis have defined privacy as" the right to let alone" and their concern about privacy was quite prompted [1]. The emerging ambiguity in information society has raised many privacy and trust issues that are context dependent. These issues will pose many challenges for policy-makers and stakeholders because people's notion of privacy and trust are different and shifting [2]. Policies are considered as a fundamental factor to provide security and privacy in applications such as, file sharing, Web browsing, Web publishing, networking, and mobile computing. Such applications demand highly accurate policies to ensure that resources remain available to authorized access but not prone to compromise. The policies of the past are not suited to deal with new challenges and we are probably entering into new era that would require developing more effective policies. There are lots of uncertainties and risks today concerning our privacy and trust. It is also seen that people are sometimes compelled in circumstances to surrender their personal data to gain something [2]. Two non-expert groups of policy authors are on the rise. First are the non-technical enterprise policy authors, typically lawyers or business executives, who have the responsibility to write policies governing an enterprise's handling of personal information [3]. Second are end-users, such as that wish to set up their own spam filters, share photographs, videos or important files with friends but wants to protect them from unwanted access [4]. It is important to continue researching better mechanisms for security and privacy policies authoring and to establishing good guidelines; because to achieve the best security goals it's crucial to obtain high quality to ensure the intended policy. This work shows the current role of privacy policy in policy management, but it is still immature in making security analysis and assessments [5]. Furthermore with this research, the interest to make the organizations flexible with respect to privacy matters, consistent over the design of policy language that could be enforceable. It may be fruitful for users if policy decisions with a higher impact were presented in a different manner. In last this would be helpful for the upcoming policy authors to understand the users` concerns and experiences in terms of privacy.

Manuscript received October 2, 2011; revised December 27, 2011.

Murtaza Hussain Shaikh is with the Norwegian University of Science and Technology (NTNU), 7448, Trondheim - Norway. He is also now in Mehran University of Engineering and Technology (MUET), 71000, Jamshoro, Pakistan. (e-mail: shaikh@stud.ntnu.no). Phone: +92-3332648626.

II. Background Realities

This section is laid down to get a good basis for specifying the ground of this area and creates a sense about the level of the users` concerns on privacy policy.

A. What are Privacy Policy and Security Trust Issues?

Privacy policies are meant to protect the privacy of the user: they need to reflect current regulations and possibly promises made to the customers. "A privacy policy is a legal document that discloses some or all of the ways a party gathers, uses, discloses and manages a customer's data. The exact contents of a privacy policy will depend upon the applicable law and may need to address the requirements of multiple countries or jurisdictions" [6]. While there is no exact universal guidance or recommendations for the content or text of specific privacy policies, a number of organizations provide example forms, templates or online consultant for this purpose [6]. Privacy policies arise further issues in comparison to access control policies, as they require a more sophisticated treatment of deny rules and conditions on context information; moreover privacy policy languages have to take into account the notion of "purpose", which is essential to privacy legislation [7]. "A subset of privacy policies are enterprise privacy policies which furthermore have to provide support to more restrictive enterprise-internal practices and may need to handle customer preferences" [7]. This means that an enterprise level privacy policies plays a vital role to increase the loyalty with the users. A good reason for supporting

enterprise privacy policies that it not only regulates access to data, but can impose some (i.e. obligations like to delete a data set within two weeks or simply notify the customers of the business firm) [7].

B. Is a Policy Context Difficult with Typical Legal Jargon?

Many researchers and experts of system security are asking the question; why do few people read the privacy policies? [8]. One common fact is simply that policies are often written in a hard and complicated language which a common user or subscriber cannot understand [8, 9]. In privacy notice research conducted by [10] the research is conducted in 2001 and in that research, 29 percent of the respondents expresses their feelings that policy contents are very difficult to read and 45 percent of respondents said that it was difficult to understand them. Another good reason subscribers have given for not understanding the policy is that they contain a lot of legal and lawful jargon [10]. In the survey by Milne [11], about 53 percent of the respondents agreed, or strongly agreed to, that privacy notices often use legal language which is very hard to understand or is confusing for most people. Same as described in [12] those policies use certain statement and distinct vocabularies which made them very hard to understand, even for the experienced reader.

C. What is the Standardization of Policy Context?

Lack of standardization of privacy policy contents is also a problem. Different websites use different ways for structuring the information in their policies. Many service operators claim that their security statement first explains what particular information they are collecting and then how they will use those details [13]. Other service operators tells where on the website they would collect personal information, and then explain what they will do to protect this information [13]. Some service operators post on their website F.A.Q (Frequently Asked Questions) format focusing on answering the most common questions that mostly asked by the users regarding their privacy [13]. There is no particular standardization adopted across the organizations / companies for comparison [12]. The ability to compare policies could be helpful in many situations (e.g. where users have a chance to select a company /organization to fulfill its requirements on privacy and security).

D. What is an Accessibility of Policy Contents?

Recent studies have found that there are accessibility issues with privacy policy [14]. A study conducted in 2009, says that in forty five different social networking sites just fifteen sites opened their privacy policies in a new window which could be blocked, interrupted or inaccessible from the mobile devices [14]. It was also found issues where a JavaScript was a requirement to access the policy in those sites the policy contents could not be saved, printed or zoomed. It was also found that only 2 pages scored perfect on a mobility access test. Location and format of the policy has also been found to be a critical issue [12]. In their problem formulation, [13] the author claimed that the link to a privacy document is often difficult to spot, often hidden at the bottom of the website in very small font. This claim is, however, not supported in a more recent study by [15], where it was found that the privacy policies examined generally had good accessibility, with a consistent location of the privacy policy at the bottom of the homepage (around 86 percent of the privacy policies) . It was found that despite the unglamorous location, the consistency provided the user with a location clue of where to find the policy [15]. A survey conducted in 2001 found that 48 percent of the respondents agreed strongly that privacy notices were easy to find [11] and only 22 percent of the users disagree to the same concept.

E. What are the Main Privacy Concerns?

The privacy threats of which people are concerned include;

1) Visit to the websites will be tracked secretly without informing the user [16].
2) E-mail ID and other confidential and personal information will be stored and used for marketing, publicity and other similar purpose without permission of the user [16].
3) Personal information will be sold to third parties /vendors without getting permission from user [16].

The advances of internet and database technologies increase information privacy threats. Data entered into forms or contained in existing databases, can be combined almost effortlessly with banking transaction records, and records of a user's every click of a mouse on internet. Privacy concerns increase further as data mining tools and services become more widely available [17]. There is a potential for fraudulent activities on the internet, as few regulatory standards exist [18]. The security of banking card information for online purchase is also incorporated with the privacy concerns. Amazon.com admitted that hackers undetected over four months have stolen about 98,000 bank card numbers. Hackers from time to time publish a list of stolen card numbers and related information over the internet [18]. The information without permission may lead to a fraud, which has very serious consequences [17]. Although personal information may not be used after collecting them, it must be noticed that keeping information is a liability for a website when it meets some good consumers or some old users that take the safeguard of their privacy seriously. The Internet based businesses should take good care of the privacy concerns because the common consumer does not really care about going through every line of policy context. Surveys show that people are more comfortable if they see privacy statement has been approved by a third party, such as Trust-E [19, 20]. To boost the e-commerce environment, information privacy concerns should be treated seriously as they are discouraging users from using the internet in shopping and services [17].

III. Principles And Guidelines

In this section we will see that different approaches to regulate privacy protection has led to a global patchwork of privacy laws, regulations and enforcement mechanisms which vary greatly from state to state, region to region, adding complexity to the privacy landscape. Many of the laws and regulations enforced today do however have something in common which is that they are based on privacy principles and guidelines developed over past 40

years.

A. Fairness and Lawfulness

This principle implies that personal information should be handled fairly and lawfully. Behind this important principle is a requirement that the data controller should respect and take into consideration the data subject's interests and reasonable expectations [24]. The data subject should not be forced to submit personal information or to accept that this information is used to other specific purposes. The data subject should be informed of the purpose of the collection of the data, and the processing of the data should be understandable [24].

B. Limitations on Collection

The basic purpose of this principle is to limit the amount of data collected to what is necessary to carry out further processing of the data which corresponds with OECD's collection limitation principle. In [24] the authors mention that there is not enough reason that the information is useful, the information must be necessary. The further processing of data should correspond with the purpose of which the data was collected for [24]. When the data is not longer necessary to fulfill the purpose they should be deleted or made anonymous [24]. This principle does also propose that individuals should be able to be anonymous in transactions with other service provider.

C. Purpose Binding

This principle means that personal information should be handled to a stated, legitimate purpose and should be handled to this purpose only. The purpose should be stated in a reasonable accurate way not later than at the time the information is collected, which complies with the purpose specification principle and the use limitation principle of OECD [24].

D. Quality of the Information

This principle is concerning the quality of the information. The information should be correct compared to what the information is supposed to represent [24]. The information should also be relevant, adequate and complete based on the purpose of which the information is to be used, and to be up to date, which correspond with the data quality principle of OECD [24].

E. The Co-determination

This principle implies that the data subject should to a certain degree be able to participate and influence other`s processing of information concerning it [24]. Persons can decide themselves if personal information about them is to be collected by others and for what purpose, unless the collection is done by the legal authority. This implies that persons can oppose to some types of processing of personal data, such as personal marketing [24]. At last, this principle implies that persons can demand that information concerning them should be deleted or corrected if the information is incorrect, incomplete or illegal to register [24].

F. Security Safeguards

The confidentiality and integrity of personal data should be protected by reasonable security safeguards [24]. Confidentiality here means protection of personal data from unauthorized access or disclosure, and protection of integrity means protection against unauthorized destruction, use and modification of personal data [24]. This principle encourages actions like use of firewalls, IDs (intrusion detection systems) etc. This principle complies with the security safeguard principle of OECD [24].

IV. Privacy Laws And Regulations

This section is highlighting the necessity to understand the complexity of the underlying legislations and regulations that form the basis for the current content and structure of privacy policies in today`s era. We will see that different approaches to regulate privacy protection has led to a global patchwork of privacy laws, regulations and enforcement mechanisms which vary greatly from state to state, region to region , adding complexity to the privacy landscape.

A. EU Data Protection Directive (EUDPD) [1995]

The EU directive on the protection of individuals with regard to the processing of personal data and on the free movement of such important data was agreed upon on the 24th of October, 1995 by the European Parliament in Brussels and the EU's Council of Ministers [25]. The directive instructs the members of EU to pass legislation which corresponds to the rules in the directive. According to article 4 of the EUDPD directive, the member countries are not allowed to pass legislation that suggests a poorer protection of privacy than what the EU directive proposes. The purpose of the directive is to harmonize the legislation of the member countries which in turn will encourage trans-border flow of personal data between member countries. The author in [25] explains clearly that that the reason for this wish is, among other factors, the desire for the internal EU market to function as good as possible. The directive introduces a minimum standard of protection of privacy which the member countries cannot deviate from. But the directive allows the countries to do small changes. Although the member countries cannot pass laws that suggest a poorer protection of privacy, the directive does not suggest any limit for how strict this legislation might be in each country. The member countries can pass laws that suggest a better protection of privacy [25]. The directive is covering both governmental and private sectors, but the directive does not cover processing which concerns the security of a state or country, including the countries' economical interests when processing is associated with questions regarding the safety of the country [25]. This means that a country can pass legislation which provides no protection of privacy as long as the processing of the personal information is concerning the safety of the country. The directive also demands that every member country establishes a regulatory agency which governs the use of personal data and makes sure the legislation is followed by (article 28th of EUDPD) and every member country is to introduce an arrangement of obligation to submit reports for every organization which whishes to handle personal data [25].

B. EU Convention for Protection Identification with Regards of Automatic Data Processing [1981]

This convention was approved on the 28th of January

1981 by the European council w.e.f 01st, October of 1985. Norway ratified the convention on 20th of February 1984 [24]. By ratifying we mean that a state or country commits to incorporate the principles of the convention. The convention establishes some minimum norms for automatic processing of personal data. Beyond that the convention does not describe any rights that individuals can employ, or demand for establishing a data inspectorate. The convention has two purposes, first to improve the protection of privacy, and second to encourage international business [24]. The reason for the last purpose is that countries like Norway had laws that restricted trans-border flows of personal data. The principal rule of this convention is that any country that has ratified the convention "shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorization trans-border flows of personal data going to the territory of another party" [26]. A restriction like this is allowed if the information is directly protected by the country of origin and the host country cannot offer the equivalent protection. The convention is political binding for the members of the European Council and therefore the convention makes up an important basis for preparations of national laws [24].

C. The Norwegian Personal Data Act (POL) [2000]

This law was passed on the 14th of April 2000 and came into force on the 1st of January 2001 [26]. his law contains a general view of the processing of personal information and it is based on the EU directives. The Norwegian Personal data Act is also referred as POL Act of Norway. The purpose of this law is to "protect the individuals against invasion of privacy by the processing of personal information" [24, 26]. It regulates all electronic processing of personal information, with no concern about how the information is stored or what kind of operations are performed on the information. This means that the law regulates the processing from the day the information is collected to the day the information is deleted [26]. The law applies to all organizations which are established in Norway, even if the processing itself is not carried out in Norway. The law does also apply to organizations established outside Norway that process personal information with the help of some remedy placed in Norway [26]. The law does also apply to organizations established outside Norway that process personal information with the help of some remedy placed in Norway [26]. According to POL, the data controller must have a legal basis for handling the information before the processing can start. This means that the data controller must either hold consent from the data subject, or the processing must be founded on some law, or the processing must be 'necessary' to fulfill some purposes that are stated by the law. The consent from the data subject should be voluntary, explicit and informed. In other words, the data subject should not be forced or fooled to give up information concerning him or her [26]. The data subject can only be forced to give up information if there is a legal basis for doing so, such as the police can force a person to state his or her name and the whereabouts in the investigation of a criminal act [24, 26].

D. Privacy Practicing of Norwegian Personal Data

According to the POL 2000, personal data cannot be used for other purposes than the purpose stated when the data was collected without the approval of the data subject or the processing is done due to legislation, which means that any organization that operates its business activity or simply does the online activity for enforcing the privacy policy must somehow manage to associate system activities on personal data to purposes, or in similar ways be able to interpret the purpose of the processing [26]. In some cases the data subject has agreed to that the data processor can use the personal data for other purposes than what the data was collected for. Any application for enforcing privacy policies must therefore be able to handle policies that may vary from data subject to data subject. And therefore the identification of the data subject is an important feature in such application [26]. The POL 2000 requires that the confidentiality and integrity of personal data are protected. An application for enforcement of privacy policies is a type of an access control system and will therefore, at least partially, contribute to the protection of the confidentiality and integrity of the personal data [26]. POL 2000 limits the period an organization can store personal information about their customers, but the Norwegian data inspectorate (Datatilsynet i Norge) may instruct the organization to take further actions to preserve the privacy of their customers.

V. Evaluation And Results

In this section we will discuss the evaluation and results of the survey and our observations related to the research theme.

A. Evaluating Results of Service Provider`s Survey

The online survey that we have conducted to investigate the service provider's point of view about the privacy policy and its impact on their subscribers. At this level of research, it was feasible to target the Norwegian service providers because; the working environment of this work was in Norway and also due to limited time constraints and resources etc. In order to get a large number of responses, we distributed our online survey to 80 large service providers that are operating in Norway. It was suitable to get the response from Norwegian Service provider because; it will show how Norwegian companies perception on the privacy policy. We have selected the companies according to their reputation in the business world and their large number of registered subscribers. Our primary target was to collect responses from the Internet / Telecommunication/ Scientific / Research sector as they often collect the sensitive data from their subscribers.

B. Categories of Participated Organization in Survey

The fig.1 is showing the different categories of the survey organizations. As it was mentioned in the previous section that our primary target was to focus on Internet / Telecommunication / Scientific / Research organization because they have a good knowledge about the privacy policy issues and they can record their response positively to our survey.

In fig. 1, we can see that majority is the internet organizations with 4% of the response, and next higher response is 3% from telecommunication organizations. Only 3% response comes from marketing / advertisement organizations. Just 2% of the response collected from scientific/research and academic organizations and 2% of the response comes from the trade / business organizations.

2% of the response was given by the energy sector and 1% of the response from financial institutions.

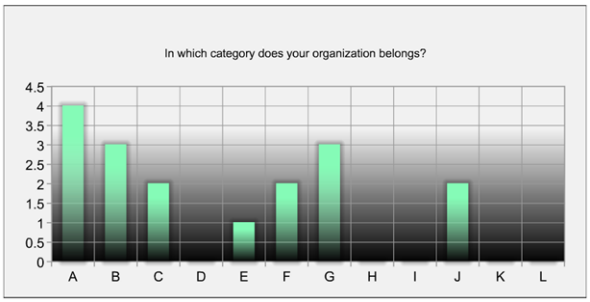

Fig. 1. Categories of participated organization.

C. Service Provider`s Location

Analyzing fig. 2, we see that most of the service providers operate inside the territory of Norway and their services are being used by the local Norwegians.

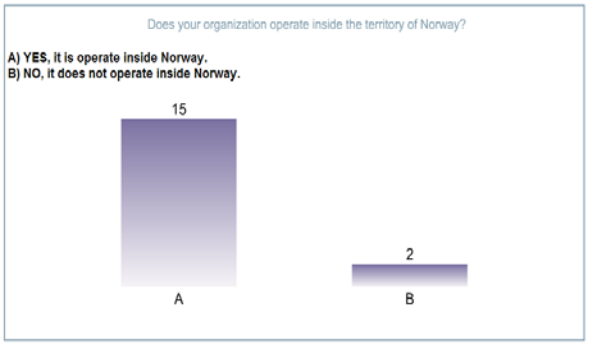

Fig. 2. Response of service provider's location and operations.

D. Service Provider`s Importance on "Privacy Policy"

By examining fig. 3, we see that 47% of the responded service providers give a strong and keen importance on the privacy policy because they know how important this is for them to acquire goodwill in terms of securing their customer`s privacy, this percentage is high among all the other responses. Next recorded response is 35% in which the service provider has given an average importance to privacy policy. Lastly 18% of the respondent service providers give a low importance on privacy policy for the subscribers.

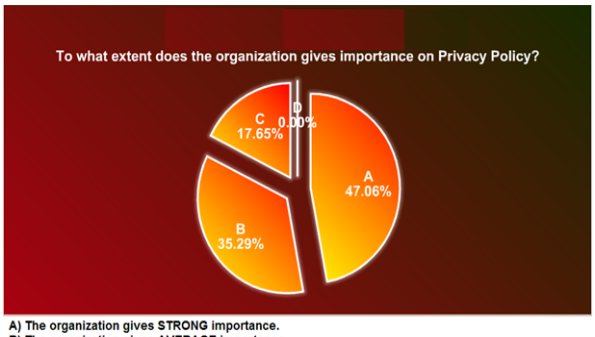

Fig. 3. Level of importance on privacy policy.

E. Standards of Privacy Regulations and Laws

From this question we have tried to investigate what standards or a regulation of privacy and its defined laws does the service provider use while collecting the personal information from the common users. In the survey we have mentioned many privacy standards and laws to see which of them are used by the Norwegian service providers.

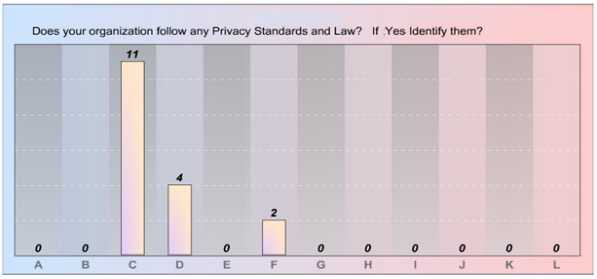

Fig. 4. Response of following privacy standards and regulations.

F. Response of Reading "Privacy Policy" from Their Subscribers

The Fig. 5 shows the response to the question on how large portion of the users read the privacy policy when they are registered. This is a service provider perspective. Just 29% of the respondent organizations think that (10 to 30 percent) users read their privacy policy. Another response given by the organization which is 29% thinks that (30 to 60 percent) users read the organization`s privacy policy. Around 24% of the respondent organizations think that (60 to 90 percent) users read the privacy policy. Finally we can see that 18% of the service providers think (below 10 percent) of their users read the privacy policy.

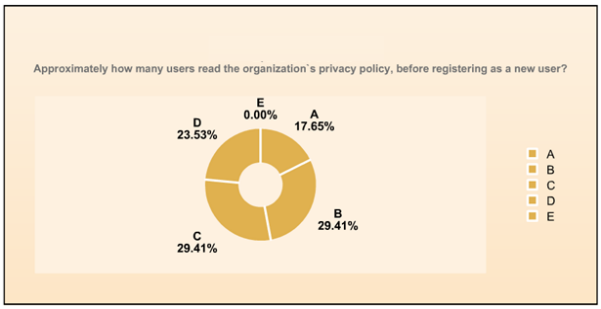

Fig. 5. Response reading the policy contents from subscribers.

G. Level of Understanding Privacy Contents for Subscriber

With the help this question, we got an idea of the level understandability of privacy contents for subscriber from the service providers' point of view. In fig. 6 a bar chart is showing that 80 percent of the respondent organizations think that *"some of contents of privacy policy deal with the legislation and they are not relevant for common users"*. While 60% of the respondent organizations think that *"privacy contents are highly relevant and they determines the user`s*

operational limitation". Finally 30% of the respondent service providers think that *"the privacy policy contents are not relevant for them and they just explain unnecessary text etc"*.

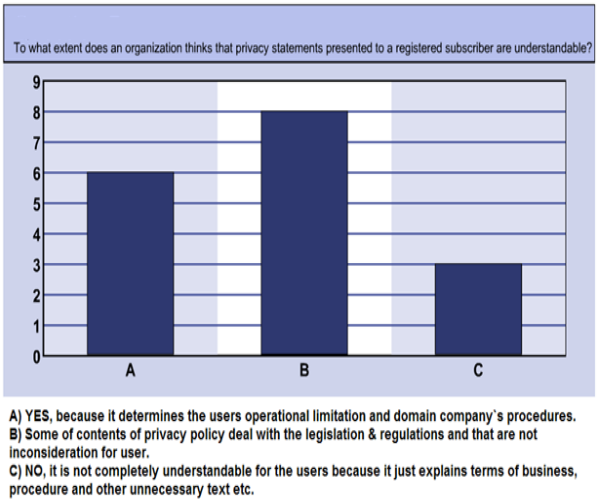

Fig. 6. Level of understanding privacy contents.

H. Any Review Body on Setting up "Privacy Policy"

We were asking from the respondent companies if they have some review body and all the respondent companies answered that they have a review committee on privacy policy. Total 6% of the respondent companies voted that they have a review body / committee on privacy policy and they amend or modify the policies "every year". As shown in fig. 7 five percent of the companies amend their privacy policy after "more than two years".

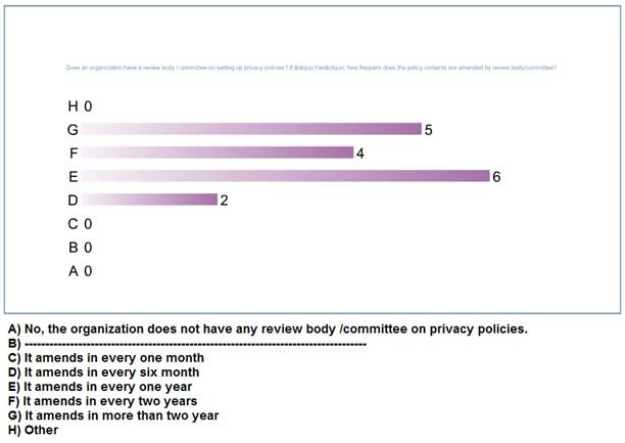

Fig. 7. Response of having review body on privacy policy.

By evaluating the graph we can observe that just 4% companies amend their privacy policy context in "every two year". Next percentage is 2 percent, showing that just few companies review their privacy contents after "every six months".

I. Retention Regulation in Service Provider Privacy Policy

The Fig. 8 shows the responses to our question about the retention regulation followed by the service provider in their defined privacy policy. The retention regulation is an important part of any privacy policy.

By analyzing the pie chart in fig. 8 we see that majority (i.e. 53 percent) of the respondent companies in Norway follow the retention regulation but there is a pre-defined time frame to follow this regulation. Next we have 47% of the respondent service providers that strictly follow the retention regulation in their privacy policy.

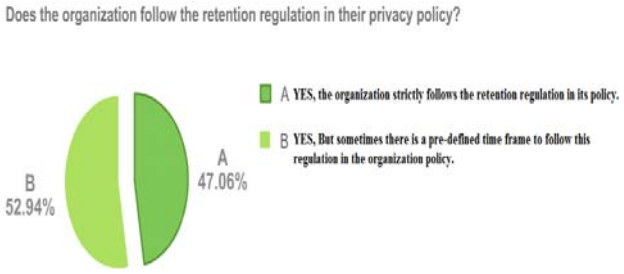

Fig.8. Response of following retention regulation.

J. Disclosure of Subscriber`s Personal Information

As explained in fig. 9 we have asked the companies about to what extent they disclose the subscribers' personal data to any 3rd party or 3rd vendor. We have got a positive response that 7 percent of the service providers are mentioning in their privacy policy that *"the organization can disclose the personal data of subscribers if the Country / State law enforcement agencies or bodies request"*.

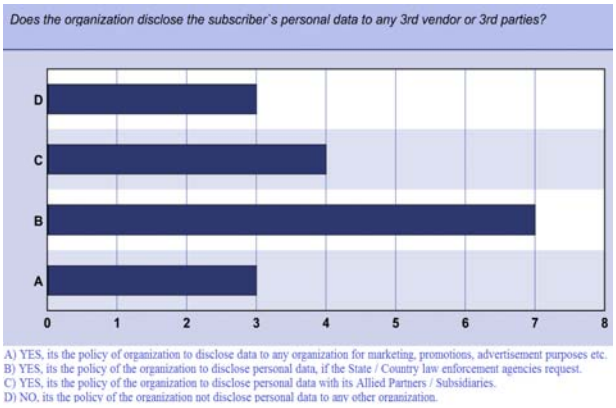

Fig. 9. Response of disclosure of personal information.

About 4 percent of the respondent service providers voted that it is in their privacy policy that *"they can disclose the personal information of their users to allied partner, collaborator or subsidiary firms etc". Nearly 3 percent of the service providers "do not disclose the subscriber`s personal data to any other organization what so ever happened and this is mentioned in their privacy policy"*. Finally, 3 percent of the respondents said that *"they disclose the personal data to any organization for marketing, promotion and for advertisement purposes etc"*.

K. Level of Building Confidence and Trust for Subscriber

The result shown in fig. 10 describes how the service providers build confidence and trust for a subscriber in terms of privacy and how they performing their operations which are trustful to their users.

Approximately 35% of the respondent service providers said that by introducing the privacy protection seals on their website they can build a strong trust and confidence for their subscribers. 23% answered to this question that to build a trust by following a strict policy statements and guidelines in their website. About 23% of the service providers take other standard protective measures. Just 18%

of the service providers are providing Https secure channel of communication to ensure the privacy of their subscribers.

Fig. 10. Level of confidence and trust for a subscriber.

L. *Response from Internet Sector*

In fig. 11, we have collected the response from the internet sector in Norway. The entire service provider follows the Norwegian personal data act of [2000] as a privacy regulation whenever they collect the personal data from the Norwegian subscribers and 17 percent of the registered users are approximately are more than 300, 0000. The internet sector is giving the high priority to the privacy policy phenomena.

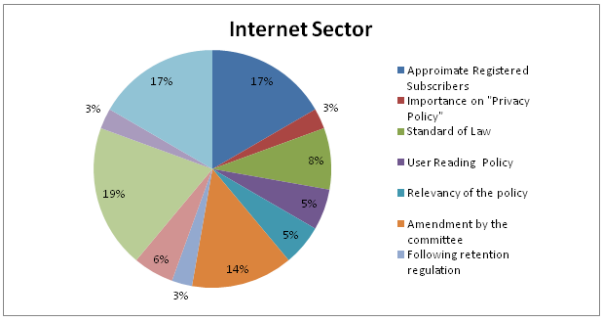

Fig. 11. Response from the Internet sector.

This sector thinks that a 30 to 60 percent of the users read their privacy statements before registering themselves as a new user. It is interesting to note that some policy contents in this sector are deal with the legislation and regulations and that are not inconsideration for user. The policy amendments are generally performed after every year. Majority of this sector companies follows a strict retention policy.

M. *Response from Telecommunication Sector*

As shown in the fig. 12, the response from the telecommunication sector of Norway. Just one service provider was operating outside the Norway. There were approximately more than 300, 0000 registered users with these service providers and they follows the Norwegian personal data act of [2000] as a standard law for collecting the personal information from there users only one service provider follows the European Union personal data directive of [1995].

Here the respondent companies give an average importance on the privacy policy phenomena, and these respondent organizations perception is that round 60 to 90 percent of their users read the privacy statements before signing up as a new user with the organization. The majority of respondent service provider also thinks that some of contents of privacy policy deal with the legislation and regulations and that are not inconsideration for user and very few thinks that regarding the understanding of their policy context that it is not completely understandable for the users because se it just explains terms of business, procedures. This respondent sector after every two years time gap amends their policy and they have a proper review committee of amending the privacy policy.

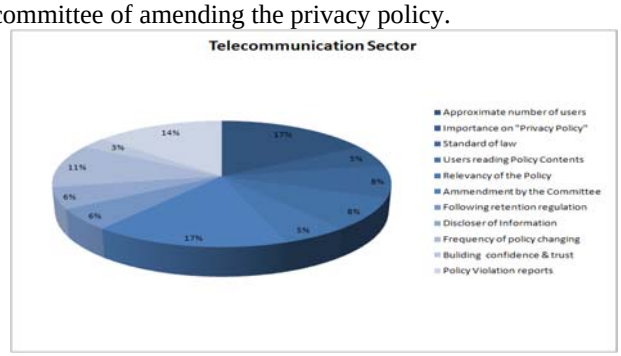

Fig. 12. Response from the telecommunication sector.

N. *Response from Scientific / Research / Academia Sector*

The fig. 13, examines the response comes from the research / academia sector from our online based survey. All the respondents are operating inside Norway. There are 2, 00000 - 250, 0000 registered users associated with this sector and all the respondent organization gives strong importance to privacy of the user and its policy contents. All the respondent organization follows the Norwegian personal data act of [2000] when the request user to enter their personal information.

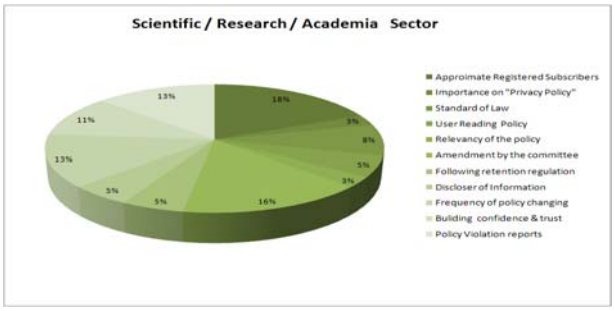

Fig. 13. Response from the scientific / research / academia sector.

It was surprising for us to see that according to the respondent organization thinks just 10 to 30 percent of the users read privacy policy and they thinks that privacy policy presented to the users are very well understandable because it determines the user's operational limitation and domain company`s procedures. These respondent organizations also disclose the user`s personal data because it is mentioned in their policy that the organization to disclose personal data, if the State / Country law enforcement agencies request and it can share the data to their allied partners, collaborated firms or their Subsidiaries.

O. *Response from Financial Sector*

We are showing in fig. 14, the response comes from the financial sector from our survey research. This financial sector purely operates in Norway and follows strictly the Norwegian personal data act of [2000]. Approximately it has more than 300, 0000 registered users and indeed the financial sector gives a very high priority on privacy of their registered users which shows a positive sign of their operations. The financial thinks that between 30 to 60

percent of the users read their privacy policy before they are using their services and this respondent sector also thinks

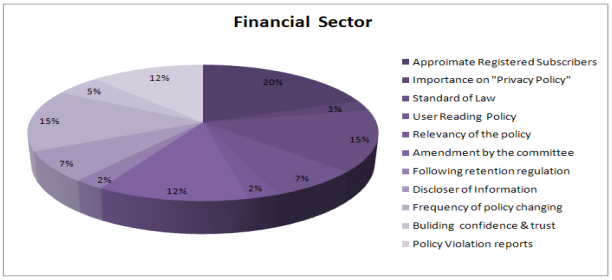

Fig. 14. Response from the financial sector.

that their privacy policies are well understandable and they purely determines the user's operational limitation and domain company`s procedures. The respondent sector amends its privacy policy every year and they follow strictly the retention regulation in their privacy policy. This sector builds a strong trust and confidence for a subscriber by providing the Https channel of communication on their official websites.

VI. Conclusion

Privacy issues have become increasingly important as the tail of information we leave behind us is rapidly growing and the potential misuse and theft of information is well recognized. To minimize the intrusion into a person's privacy caused by the collection, storage and use of the personal data, the field of data security and protection has emerged. An important and serious part of the data protection is to communicate the laws and regulations regarding the usage of the personal data of users, and the privacy policy serves as a path in this context. Privacy policies have the motivation of increasing the user's general confidence in sharing personal information, but most of the research has shown that they have failed to achieve this prospect. A very few users actually read the policies and understand them. Questions have been raised regarding whether they have any effect on the user's trust and confidence at all. Alternative ways of presenting privacy policy and its related regulations to the common users are urgently needed. To be able to propose an innovative approach to present the policy, one needs to explore the current status of the privacy policies and their related aspects. The purpose of this work has been to conduct a survey to lay a strong foundation for further work on the privacy policies and impact on the social and moral grounds. We therefore have conducted an explorative study and read related work on this topic in order to explore some relevant problem definitions. In conducting this research we also saw that any innovative approach on presenting privacy policy to the user are limited by varying enforcement mechanisms, and that again tries to limit the further research on this important issue.

Acknowledgment

I would like to express my gratitude Professor. Torbjørn Skramstad of Department of Computer and Information Sciences (IDI), Norwegian University of Science and Technology (NTNU) for all the help and support in writing this paper. Many thanks to my family and especially to my mother Mrs.Naseem Ahsan Shaikh, who`s prayers, love and trust on me to have a bright academic career in my life.

References

[1] Warren, Samuel, and Louis D.Brandeis, *"The Right to Privacy,"* Harvard Law Review Association. vol.iv, No.5.

[2] David.W, Serge. G, and Michael. F, "Privacy, trust and policy-making: Challenges and responses," *Computer Law and Security Review*, 25- 2009. Elsevier Ltd Publication. vol, 69-83. 2009.

[3] J. Karat, C.-M. Karat, C. Brodie, and J Feng, "Privacy in information technology: Designing to enable privacy policy management in organizations," *International Journal of Human-Computer Studies*, 2005.

[4] X. Cao, L Iverson, Intentional access management: "Making access control usable for end-users," In Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS 2006), New York, NY, pp. 20–31. *ACM Press*, New York, 2006.

[5] C. Brodie, C.M.Karat, J.Karat and J.Feng, Usable Security and Privacy: "A case study of developing privacy management tools," In SOUPS `05: proceeding of the 2005, Symposium on usable privacy and security ACM, New York, 2006.

[6] Wikipedia the Free Encyclopedia. *"Privacy Policy."* [Online]. Available: http://www.wikipedia.org. Accessed on September, 26th, 2010.

[7] A Piero, L. Juri, O. Daniel, and S. Luigi, "Rule-based policy representations and reasoning," *Springer*.USA. 2007.

[8] H. Simth, S. Milberg, and S. Burke, "Information privacy. Measuring individuals concerns about organization practice," MIS Quarterly, 20(2): 167-196, 1996.

[9] Wham. T. "*Transcript of the Federal Trade Commission USA Workshop on Information Privacy. Measuring individuals Concerns about Organization Practices.*" 2001. [Online]. Available: http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm

[10] Harris Interactive. *"Identity Theft: New Survey and Trend Report."* 2001. [Online]. Available: http://identitytheft.lifetips.com /cat/65329/identity-theft-statistics /index. html

[11] Milne, M.J, "The culnan-milne survey on consumers and online privacy notices: Summary of responses," In Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices, pp. 47-54, 2001.

[12] A. Anton, J. Earp, Q. He, W. Stufflebeam, D. Blochini, and C. Jensen, "Financial privacy policies and the need for Standardization," IEEE Security and privacy, 2(2), pp. 36-45, 2004.

[13] D. Bolchini, Q.He, A.L. Anton, W.H. Stufflebeam, "I need it now! Improving websites usability by contextualization privacy policies," In *ICWE*, pp. 31-44, 2004.

[14] J. Bonneau, and S. Preibusch, "The privacy jungle: On the market for data protection in social networks," In the Eight Workshop on the Economics of Information Security (WEIS-2009).

[15] P.G. Kelley, J. Bresee, L. F. Cranor, and R.W. Reeser, "A nutrition label for privacy," In *Proceedings of the 5th Symposium on Usable Privacy and Security SOUPS*, 09-2009. [Online]. Available: http://www.portal.acm.org/citation.cfm?doid=1572532

[16] Matt Bishop, "Computer security: art and science," Addison-Wesley Professional Publication December12th, 2002, USA.

[17] Chung.W,Paynter.J, "Privacy issues on the internet", *35th Hawaii International Conference on System Sciences*, USA 2002.

[18] W. Hancock, "Cookies on your hard-drive," *American Agent and Broker.69* (6): 8-10. June 1997, USA

[19] M. Krauss, "Don't kid yourself-consumers do pay attention to privacy," *Marketing News*, 34 (5), 13.February 28th, 2000 USA.

[20] TrustE. [Online]. Available: http://www.truste.org

[21] D. Meinert, D. Peterson, J.Criswell, and M. Crossland, "privacy policy statements and consumer willingness to provide personal information," *Journal of Electronic Commerce in Organizations*, 4:1-17, 2006.

[22] G. Milne, M.J Culnan, "Strategies for reducing online privacy risks. Why consumers read, online privacy notices," *Journal of Interactive Marketing*, 18(3), 2004.

[23] F. Belanger, J. Hiller, and W. Smith, "Trustworthiness in electronic commerce. The role of privacy, security and site attributes," The *Journal of Strategic Information Systems*, 11 (3-4), pp.245-270, 2002.

[24] D. W. Schartum and L. A. Bygrave, "Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger," Fagbokforlaget, Norway, 2004.

[25] EUDPD, "The EU directive on the protection of individuals with regard to the Processing of personal data and on the free movement of such data," vol. 95/46/EC, 1995.
[26] The Norwegian Personal Data Act POL, "Lov om behandlig av personopplysninger," vol. LOV-2000-04-14-31 Norway, 2000.

Murtaza Hussain Shaikh is 26 years old author from Pakistan and has earned Master`s student in (Information Systems Engineering) from Norwegian University of Science and Technology (NTNU), Norway in 2011 and another Master`s degree in (Science and Technology Policy) in 2009 from Mehran University of Engineering and Technology (MUET), Pakistan in 2009. He got his Bachelor`s degree in (Software Engineering) from University of Sindh, Pakistan in 2006 and another in (Arts and Economics) from Allama Iqbal Open University, Islamabad, Pakistan in 2008. His current research interests include IS Security, Technological Law and Policy Making, IT Systems operations and Maintenance, Cyber Crimes and Cyber Security issues. He has a research and teaching experiences in Computer Science in different Pakistan`s Universities and Colleges. He has authored and co-author many research articles in International Journals and Conferences. He is also affiliated and member of professional associations /committees like IACSIT –Singapore, IAENG – Hong Kong, PCB- Pakistan, and IJPA – USA.